



06-23-04

IFW

Express Mail Label No.

Dated: _____

Docket No.: 20193/0201145-US0
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Wieland Fischer et al.

Application No.: 10/825,582

Confirmation No.: N/A

Filed: April 14, 2004

Art Unit: N/A

For: METHOD AND DEVICE FOR
CALCULATING A RESULT OF AN
EXPONENTIATION

Examiner: Not Yet Assigned

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is filed within three months of the U.S. filing date (37 CFR 1.97(b)(1)).

A copy of each document on the PTO/SB/08 is attached. Pursuant to the Notice issued by the United States Patent and Trademark Office dated July 11, 2003 waiving the requirements of 37 C.F.R. 1.98(a)(2)(i), copies of the United States Patents on PTO/SB/08a are not submitted.

Document DE 693 29 929 T2 is not in the English language. In accordance with 1.98(c),
Applicant states:

The requirement for concise explanation of relevance of document DE 693 29 929 T2 is satisfied by the attached translation of the abstract (see MPEP § 609 A(3)).

In accordance with 37 CFR 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR 1.56(a) exists. In accordance with 37 CFR 1.97(h), the filing of this Information Disclosure statement shall not be construed to be an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 CFR 1.98 and the Examiner is respectfully requested to consider the listed references.

The Commissioner is authorized to charge any deficiency of up to \$300.00 or credit any excess in this fee to Deposit Account No. 04-0100.

Dated: June 21, 2004

Respectfully submitted,

By  *Laura C. Brutman*
(53,970)

Laura C. Brutman
Registration No.: 38,395
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(212) 527-7700
(212) 753-6237 (Fax)
Attorneys/Agents For Applicant



PTO/SB/08a/b (08-03)

Approved for use through 07/31/2006. OMB 0651-0031
 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/B/PTO				Complete If Known	
				Application Number	10/825,582
				Filing Date	April 14, 2004
				First Named Inventor	Wieland Fischer
				Art Unit	N/A
				Examiner Name	Not Yet Assigned
Sheet	1	of	1	Attorney Docket Number	20193/0201145-US0

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
AA**	US-4,532,638-B1	07-30-1985	Lagger et al		
AB**	US-6,125,445-B1	09-26-2000	Arditti et al.		

FOREIGN PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)			
BA	WO-00/25204-A1	05-04-2000	Vanstone et al.		
BB	DE-693 29 929-T2	09-27-2001	Gressel et al.		x

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. **CITE NO.: Those patent(s) or publication(s) which are marked with an double asterisk ("*) next to the Cite No. are not supplied because they were previously cited by or submitted to the Office in a prior application relied upon in this application for an earlier filing date under 35 U.S.C. 120. ¹Applicant's unique citation designation number (optional). ²See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS					
Examiner Initials	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			
	CA	Oswald E et al: "Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks"; Cryptographic Hardware and Embedded Systems, 3rd International Workshop, CHES 2001, Paris, France, May 14-16, 2001 Proceedings, Lecture Notes in Computer Science, Berlin, Springer, DE, Vol. 2162, pages 39-50, ISBN: 3-540-42521-7.			
	CB	Kocher P: "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems"; Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, CA, August 18-22, 1996, Proceedings of the Annual International Cryptology Conference (CRYPTO), Berlin, Springer, DE, Bd. CONF. 16, August 1996, pages 104-113, ISBN: 3-540-61512-1.			
	CC	"Handbook of Applied Cryptography", Menezes, van Orschot, Vanstone, CRC Press, 1996.			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹Applicant's unique citation designation number (optional). ²Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature	Date Considered
--------------------	-----------------



Application No. (if known): 10/825,582

Attorney Docket No.: 20193/0201145-US0

Certificate of Express Mailing Under 37 CFR 1.10

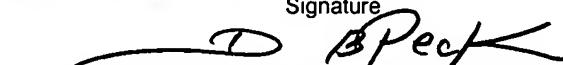
I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. EV418267552-US in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on June 21, 2004
Date



Signature



Typed or printed name of person signing Certificate

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Information Disclosure Statement (2pp)
PTO/SB/08a with five documents
Return Receipt Postcard